REMARKS

The Examiner is thanked for the performance of a thorough search and for the telephone interview conducted on July 11, 2008. By this response, Claims 1, 3-7, 9-10, 14, 16, 17-20, 24-26, 28-37, and 39-42 have been amended. Claims 43 and 44 have been added. No claims have been canceled. Hence, Claims 1–14, 16–20, 24–26, and 28-44 are pending in this application.

All issues raised in the Office Action are addressed hereinafter.

I. INTERVIEW SUMMARY

Applicants thank the Examiner for the telephone interview conducted on July 11, 2008. Examiner Shaifer Harriman, Dant B and his supervisor, Examiner Zand, represented the USPTO. Applicants were represented by Karl T. Rees. The parties discussed Claim 14's recitation of a "malicious act," the suggestion and motivation to combine the cited references, and possible amendments to Claim 1. No agreement on the allowability of Claim 14 was reached. However, the Examiner was of the opinion that the proposed amendments to Claim 1 would overcome the cited references. The Examiner also agreed to provide, in writing, his explanation of the suggestion and motivation to combine the references in the next office action.

II. CLAIM REJECTIONS BASED ON 35 U.S.C. § 103

A. Obviousness under 35 U.S.C. § 103(a): Thomsen and Renda.

Claims 1-42 were rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over Thomsen *("Thomsen")* U.S. Patent No. 7,194,004 B1, in view of Renda, et al. *("Renda")* U.S. Patent No. 7,127,524 B1. Applicants traverse the rejection. Reconsideration is respectfully requested.

INDEPENDENT CLAIM 14

Among other benefits, Claim 14 allows for the temporary quarantining of a user of a network device that triggers a security event until the nature of that security event can be

established. Quarantine is accomplished by means of forcing the user into an elevated risk group, as well as forcing the network device on to a security-restricted subnet for suspected malicious users.

Claim 14 does not require completely blocking a quarantined user from the network. For example, while on the security-restricted subnet, the user may still be provided limited access to the network. From a practical standpoint, the user might not even notice the quarantine.

Claim 14 also recites features that allow for eventual resolution to the quarantine. More specifically, Claim 14, as set forth in the listing of claims, clarifies that the method features, among other elements:

> determining whether a **malicious act** caused the security event;
> if a malicious act caused the security event, then providing information about the security event or malicious act to a security decision controller;
> if a malicious act did not cause the security event, then **removing the user from the elevated risk group**.

Security events may be caused by both malicious acts (e.g. deliberate denial of service attacks) and benign acts (e.g. user errors). The above-quoted features of Claim 14 facilitate the return of a quarantined user to a normal operating mode in the event that the security event is determined to have been caused by a benign act. On the other hand, the above-quoted features facilitate further security actions (e.g. completely blocking network access for the device) in the event that the security event is determined to have been caused by a malicious act.

For at least the following reasons, the above-quoted features are neither taught nor suggested by the cited references:

(1) The references do not disclose "determining whether a malicious act caused the security event"

Neither of the cited references teaches or suggests "determining whether a malicious act caused the security event," as recited in Claim 14. The Office Action alleges that *Thomsen* teaches such a step at col. 5, lines 54–65, col. 11, lines 62–63, and col. 12, lines 4–9. The Office Action is in error.

These passages of *Thomsen* disclose placing a device on an untrusted subnet in the event of an authentication failure. The Office Action alleges that an authentication failure is a "security event" within the meaning of Claim 1. However, the Office Action does not specifically allege any element of *Thomsen* that corresponds to the "malicious act" of Claim 14. Nor does the Office Action specifically allege any step of *Thomsen* that corresponds to "determining whether a malicious act caused the security event."

Based on the interview of July 11, 2008, Applicants' understand that the Office contends that *Thomsen*'s authentication failure is also a "malicious act" within the meaning of Claim 14. This interpretation is unsupported and conflicts with the ordinary meaning of "malicious." An authentication failure may or may not have been caused by a malicious act. For example, it may instead be caused by a benign user error, such as a forgotten password. Whereas *Thomsen* indiscriminately and permanently places devices that fail authentication on to an "untrusted network," Applicants propose placing a device that triggers a security event on to a restricted access network only until it is determined whether or not the security event was caused by a malicious act.

Furthermore, Claim 14 would not make sense if an authentication failure is both a security event and a malicious act. Simple word-substitution illustrates the problem—a process would not "determine[e] whether a[n] [authentication failure] caused the [authentication failure]."

Thus, *Thomsen*'s authentication failure does not teach or suggest a "malicious act." Nor does *Thomsen* in any way teach or suggest "determining whether a malicious act caused the security event" within the meaning of Claim 14. This element is also missing from *Renda*. In fact, the Office Action did not even allege that *Renda* disclosed or suggested this element.

(2) The references do not disclose "if a malicious act caused the security event, then providing information about the security event or malicious act to a security decision controller"

Also, neither of the cited references teaches or suggests a step of "if a malicious act caused the security event, then providing information about the security event or malicious act to a security decision controller," as recited in Claim 14. Again, the Office Action alleges that

Thomsen teaches such a step at col. 5, lines 54–65, col. 11, lines 62–63, and col. 12, lines 4–9. This is incorrect.

As mentioned previously, these passages of *Thomsen* disclose only that one may place a device on an untrusted subnet in the event of an authentication failure. Not only do these passages fail to describe a malicious act that caused this alleged security event, these passages fail to disclose that one may forward information to a security decision controller about the security event if the security event was caused by a malicious act.

This element is also missing from *Renda*. In fact, the Office Action did not even allege that *Renda* disclosed or suggested this element.

(3) The references do not disclose "if a malicious act did not cause the security event, then removing the user from the elevated risk group"

Furthermore, neither of the cited references teaches or suggests "if a malicious act did not cause the security event, then removing the user from the elevated risk group," as recited in Claim 14. Again, the Office Action alleges that *Thomsen* teaches such a step at col. 5, lines 54–65, col. 11, lines 62–63, and col. 12, lines 4–9. Again, this is incorrect.

As mentioned previously, these passages of *Thomsen* disclose only that one may place a device on an untrusted subnet in the event of an authentication failure. The passages say nothing about, after placing a device on an untrusted subnet, subsequently returning the device to a trusted subnet if the authentication failure was not caused by a malicious act.

This element is also missing from *Renda*. In fact, the Office Action did not even allege that *Renda* disclosed or suggested this element.

For at least the foregoing reasons, the combination of *Thomsen* and *Renda* fails to teach or suggest at least one feature of independent Claim 14. Therefore, the combination of *Thomsen* and *Renda* does not render Claim 14 obvious under 35 U.S.C. § 103. Reconsideration is respectfully requested.

INDEPENDENT CLAIM 1

Claim 1, as set forth in the listing of claims, clarifies that the method features, among other elements:

in a security controller that is coupled, through a network, to a network device having a first network address assigned from a first subset of addresses within a first specified pool associated with normal network users:

determining a user identifier associated with the network device that has caused a security event in the network;

in response to the security event, causing the network device to acquire a second network address that is selected from a second subset of addresses within a second specified pool associated with suspected malicious network users;

wherein the security event is an event that indicates at least one of: a possible denial of service attack, possible IP address spoofing, extraneous requests for network addresses, and possible MAC address spoofing;

wherein the second subset of addresses is different from the first subset of addresses; and

configuring one or more security restrictions with respect to the second network address.

The combination of *Thomsen* and *Renda* fails to teach or suggest a number of features of Claim 1.

(1) The references do not disclose "a security event" as recited in Claim 1

Claim 1 recites a "security event," in response to which a network device associated with the security event is caused "to acquire a second network address." The Office Action alleges that *Thomsen*'s authentication failure, as discussed at col. 5, lines 54–65, col. 11, lines 62–63, and col. 12, lines 4–9, is such a security event.

Claim 1 presently clarifies that the security event of Claim 1 does not include an authentication failure. More specifically, Claim 1 recites that "the security event is an event that indicates at least one of: a possible denial of service attack, possible IP address spoofing, extraneous requests for network addresses, and possible MAC address spoofing."

Thus, *Thomsen*'s authentication failure does not teach or suggest the security event of Claim 1. Nor does any other element of *Thomsen* or *Renda* teach or suggest the security event of Claim 1.

(2) The references do not disclose causing a network device "having a first network address" to "acquire a second network address"

Claim 1 recites "in response to the security event, causing the network device to acquire a second network address." Significantly, this network device already has a "first network address assigned from a first subset of addresses within a first specified pool associated with normal network users." Neither of the cited references teaches or suggests causing such a device to subsequently receive a second network address.

The Office Action alleges that *Thomsen* teaches such a step in col. 5, lines 54–65, col. 11, lines 62–63, and col. 12, lines 4–9. The Office Action is in error. Although these passages of *Thomsen* disclose that one may place a device on an untrusted subnet in the event of an authentication failure, the device placed on the untrusted subnet cannot be considered to have been assigned a "second network address" because the device never had a "first network address assigned from a first subset of addresses within a first specified pool associated with normal network users."

In fact, since *Thomsen*'s device has not been authenticated on the network, it would have been impossible for *Thomsen*'s device to have a "first network address assigned from a first subset of addresses within a first specified pool associated with normal network users." Thus, it could not then be assigned a "second network address."

This element is also missing from *Renda*. In fact, the Office Action did not rely upon *Renda* for teaching or suggesting this element.

(3) The references do not disclose a network device "having a first network address" causing a security event

For the same reasons, *Thomsen* fails to disclose a security event caused by a network device "having a first network address assigned from a first subset of addresses within a first specified pool associated with normal network users." At the time of *Thomsen*'s authentication failure—the alleged security event—the device that caused the authentication failure would not have had a "first network address," and therefore could not be considered to be the network device of Claim 1. *Thomsen* further fails to disclose a security event within the meaning of

Claim 1, because the authentication failure does not come from a network device having said first network address.

For at least the foregoing reason, the combination of *Thomsen* and *Renda* fails to teach or suggest at least one feature of independent Claim 1. Therefore, the combination of *Thomsen* and *Renda* does not render Claim 1 obvious under 35 U.S.C. § 103. Reconsideration is respectfully requested.

INDEPENDENT CLAIMS 18–20 AND 24–26

Independent Claims 18–20 and 24–26 also recite features argued above with relation to Claims 1 or 14, although Claims 18–20 and 24–26 are expressed in another format. Because each of Claims 18–20 and 24–26 has at least one of the features described above for Claims 1 or 14, Claims 18–20 and 24–26 are therefore allowable over the combination of *Thomsen* and *Renda* for at least one of the same reasons as given above for Claims 1 or 14. Reconsideration is respectfully requested.

DEPENDENT CLAIMS 2, 6–13, 16–17, AND 28-42

Each of Claims 2, 6–13, 16–17, and 28-42 depends from one of Claims 1, 14, 18–20, or 24–26, and includes the above-quoted features of its parent claim by dependency. Thus, the combination of *Thomsen* and *Renda* also fails to teach or suggest at least one feature found in Claims 2, 6–13, 16–17, and 28-42. Therefore, the combination of *Thomsen* and *Renda* does not render obvious Claims 2, 6–13, 16–17, and 28-42. Reconsideration of the rejection is respectfully requested.

In addition, each of Claims 2, 6–13, 16–17, and 28-42 recites at least one feature that independently renders it patentable. However, to expedite prosecution in light of the fundamental differences already identified, further arguments for each independently patentable feature of Claims 2, 6–13, 16–17, and 28-42 are not provided at this time. Applicants reserve the right to further point out the differences between the cited art and the novel features recited in the dependent claims.

DEPENDENT CLAIMS 3–5

Each of Claims 3–5 are presently amended to depend from newly added independent Claim 44, and are patentable for at least the same reasons that Claim 44 is patentable.

In addition, each of Claims 3–5 recites at least one feature that independently renders it patentable. For instance, **Claim 3** recites "resetting a port that is coupled to the network device to prompt a user to command the network device to request a new network address using DHCP." In this manner, a router implementing the steps of Claim 3 may, without waiting for a DHCP lease to expire, force a device that caused a security event to acquire a network address from the quarantined subnet.

The Office Action alleges that such a step is disclosed in *Thomsen* at col. 8, lines 12–14 and col. 10, lines 62–64. The Office Action is in error. These passages say nothing about "resetting a port."

To expedite prosecution in light of the fundamental differences already identified, further arguments for each independently patentable feature of Claims 3–5 are not provided at this time. Applicants reserve the right to further point out the differences between the cited art and the novel features recited in the dependent claims.

III. ADDED CLAIMS / AMENDMENTS

The added claims and amendments to the claims do not add any new matter to this application. The amendments to Claim 1 are supported by at least ¶¶ [0003]–[0004] of the Specification. The amendments to the remaining claims address informalities. The amendments to the claims were made to improve the readability and clarity of the claims and not necessarily for any reason related to patentability.

Claims 43 and 44 have been added. Claims 43 and 44 are supported by at least ¶¶ [0042]–[0043] of the Specification. Claims 43 and 44 therefore do not introduce any new subject matter.

Claim 43 is patentable over the cited references for at least the same reasons as Claim 1, from which it depends. Claim 44 is patentable over the cited references for at least reasons (2) and (3) presented with respect to Claim 1. Moreover, Claim 44 is patentable for at least the

reasons that none of the references disclose "performing an action that causes the network device to request a new network address." Thus, in both references, a router would have no method for forcing a network device that caused a security event on to a different subnet. Rather, the router would have to wait for the device to request a new address at the end of its current lease.

IV. CONCLUSION

For the reasons set forth above, all of the pending claims are now in condition for allowance. The Examiner is respectfully requested to contact the undersigned by telephone relating to any issue that would advance examination of the present application.

A petition for extension of time, to the extent necessary to make this reply timely filed, is hereby made. If applicable, a check for the petition for extension of time fee and other applicable fees is enclosed herewith. If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,
HICKMAN PALERMO TRUONG & BECKER LLP

Date: July 14, 2008

/KarlTRees#58983/
Karl T. Rees, Reg. No. 58,983

2055 Gateway Place, Suite 550
San Jose, CA 95110

(408) 414-1233

Facsimile: (408) 414-1076